



Customer Firewall Procedures

EFFECTIVE DATE: 07/01/2003

PURPOSE: Establish the Virginia Information Technologies Agency (VITA) customer security procedures for obtaining firewall access; requesting firewall exemptions; and performing periodic security reviews of firewall exemptions.

SCOPE: All VITA Customers

STATEMENT OF POLICY: VITA provides a custodial data center environment for agency information processing of data files and programs, including customer data back up, and disaster recovery. As custodian, VITA is required to ensure only validated access to customer files. VITA undergoes periodic audits to ensure compliance with firewall access procedures. VITA cannot exempt agencies from firewall authentication without customer written assurance that their authentication procedures are in place and operating to the highest level of security.

VITA's firewall, and/or the customer agency's firewall must, without exception, authenticate all customer access attempts to maintain the highest level of security for data and programs. All firewall exemptions will be subject to periodic VITA security reviews.

Firewall access violations – (unauthorized access) will result in immediate forfeiture of firewall access privileges.

PROCEDURE: **Requesting Firewall Access:**

1. Requesting customer agencies must be a registered VITA customer. To register see VITA Form, Billing Account Request form ACTREQv2 at <http://www.vita.virginia.gov/misforms/forms/ACTREQv2.cfm>.
2. Customer agency Security Officer(s) must be registered with VITA's Security Services Office. To register, a signed letter from the agency CIO or Primary Agency Security Officer should be sent to Benny Ambler, Acting Director of VITA Security Services Office, 110 South Seventh Street, Richmond, Virginia 23219.
3. Once registered, the customer agency Security Officer should complete either the DIT03-004IBM (for IBM access) form or the DIT003-004UNI (for Unisys access) form, which are located on VITA's website at http://www.vita.virginia.gov/misforms/nav/Sort_File.cfm and mail the completed form to the address listed above or fax to VITA's Security Services Office at 804-371-5649.
4. VITA's Firewall Administrator, or assistant, will process the form and contact the Customer Agency's Security Officer with established passwords.

Exemptions

Alternative user authentication (e.g., Private networks, VPN, etc.) may provide trusted access and may allow firewall exemptions. The Director of the VITA Security Services Office, on a case-by-case basis, will review and formally approve each exemption. For exemption requests, complete and submit the VITA Firewall Exemption Letter located at <http://www.vita.virginia.gov/docs/psg/firewallExLetter.pdf>.

VITA Security review of exempted IP addresses – VITA's Security Services Office will periodically perform reviews of exempted firewall IP addresses (e.g., used for printer, etc.) to ensure trusted relationships are being maintained. Customer agencies are required to keep accurate and up-to-date records identifying all exempted IP addresses and communicating all exempted IP addresses being used to the VITA Security Services Office.

AUTHORITY

REFERENCE: Executive Order 51; Office of the Governor, Implementing Certain Recommendations by the Governor's Commission on Information Technology.

Executive Order 65(00); Implementing Electronic Government in the Commonwealth of Virginia.